

AWS DOCUMENTATION (VPC-peering connections with different region)

Creating the VPC and Subnets in the Singapore Region

1)CREATE THE VPC IN SINGAPORE REGION

Step I : Select the region and go to VPC service.

Step II : Click on create VPC.

Your VPCs (1) Info					Refresh	Actions ▼	Create
<input type="text" value="Search"/>							
<input type="checkbox"/>	Name ▼	VPC ID ▼	State ▼	IPv4 CIDR			
<input type="checkbox"/>	-	vpc-0cc9500ccaeab4b55	✓ Available	172.31.0.0/16			

Step III : Select VPC only.

Step IV : Provide name and IPV4 CIDR for the VPC.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

vpc-a

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

Step V : Click the Create VPC.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional

Q Name X Q vpc-a X Remove tag

Add tag

You can add 49 more tags

Cancel Create VPC

Automatically route table is created give it name.

Route tables (1/2) Info

Find resources by attribute or tag

< 1 > ⚙

	Name	Route table ID	Explicit subnet associ...	Edge associations
<input type="checkbox"/>	-	rtb-01524717b5b59789d	-	-
<input checked="" type="checkbox"/>	<div>Edit Name</div> <div>vpc-a</div>	rtb-0d258307fecddd287	-	-

Cancel Save

2) CREATE SUBNETS

Step I : click on Subnets and then create Subnet.

Subnets (3) Info

Find resources by attribute or tag

< 1 > ⚙

Create subnet

	Name	Subnet ID	State	VPC
<input type="checkbox"/>	-	subnet-0a635732791e21716	✓ Available	vpc-0cc9500ccaab4b55
<input type="checkbox"/>	-	subnet-031ae7bff9e8ff4ce	✓ Available	vpc-0cc9500ccaab4b55
<input type="checkbox"/>	-	subnet-010b8438fc30a58ed	✓ Available	vpc-0cc9500ccaab4b55

Step II : Select the newly created subnet.

Step III : Create a public subnet:

Enter subnet Details(name, availability zone,IPv4 CIDR block)

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block

256 IPs

< > ^ v

▼ Tags - optional

Cancel

Create subnet

Step IV : Create private subnet:

Repeat same process for private subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block

256 IPs

< > ^ v

Cancel

Create subnet

3)CONFIGURE SUBNET SETTINGS

Step I : Enable the auto- assign public IPv4 address for the public subnet.

Subnets (1/5) [Info](#)

<input type="checkbox"/>	Name	Subnet ID	State
<input type="checkbox"/>	-	subnet-0a635732791e21716	✓ Available
<input type="checkbox"/>	-	subnet-031ae7bff9e8ff4ce	✓ Available
<input type="checkbox"/>	-	subnet-010b8438fc30a58ed	✓ Available
<input checked="" type="checkbox"/>	pub_subnet	subnet-00abb24f16b11e1a8	✓ Available

Actions [▲](#)

Create subnet

View details

Create flow log

Edit subnet settings

Edit IPv6 CIDRs

Edit network ACL association

Edit route table association

Edit CIDR reservations

Share subnet

Manage tags

Delete subnet

subnet-00abb24f16b11e1a8 / pub_subnet

Auto-assign IP settings [Info](#)

Enable AWS to automatically assign a public IPv4 or IPv6 address to a new primary network interface for an instance in this subnet

☒ Enable auto-assign public IPv4 address [Info](#)

4)CREATE AND ATTACH GATEWAY

Step I : Create the Internet Gateway.

Internet gateways (1) [Info](#)

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	-	igw-0e1f41f6cb5b63ead	✓ Attached	vpc-0cc9500ccaeab4b5

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key



Value - optional



Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Step II : Attach the internet Gateway to the VPC.

[VPC](#) > [Internet gateways](#) > igw-05823b44bf3fe9eaa

igw-05823b44bf3fe9eaa / vp_gate

Details [Info](#)

Internet gateway ID



igw-05823b44bf3fe9eaa

State



Detached

VPC ID

-

Owner



767

[VPC](#) > [Internet gateways](#) > Attach to VPC (igw-05823b44bf3fe9eaa)

Attach to VPC (igw-05823b44bf3fe9eaa) [Info](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.



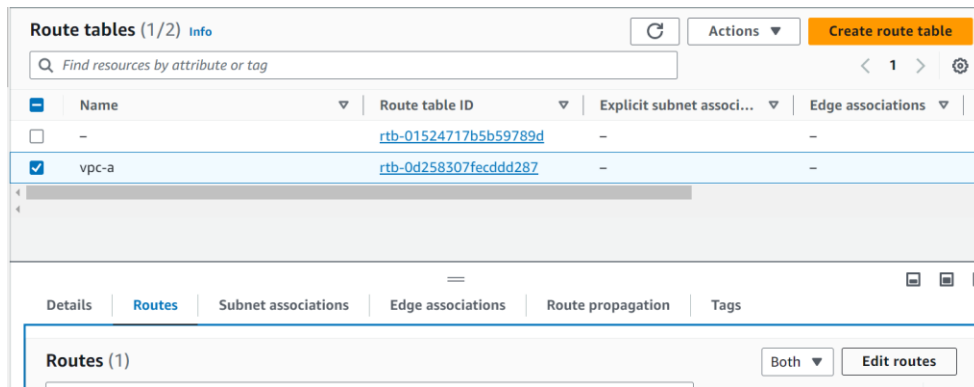
► AWS Command Line Interface command

Cancel

Attach internet gateway

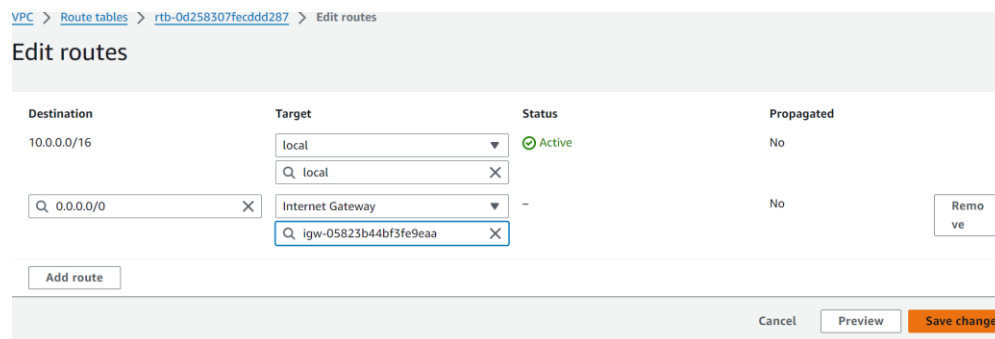
5)UPDATE ROUTE TABLE

Step I : Go to Route Tables.



Step II : Edit routes to add an internet gateway route.

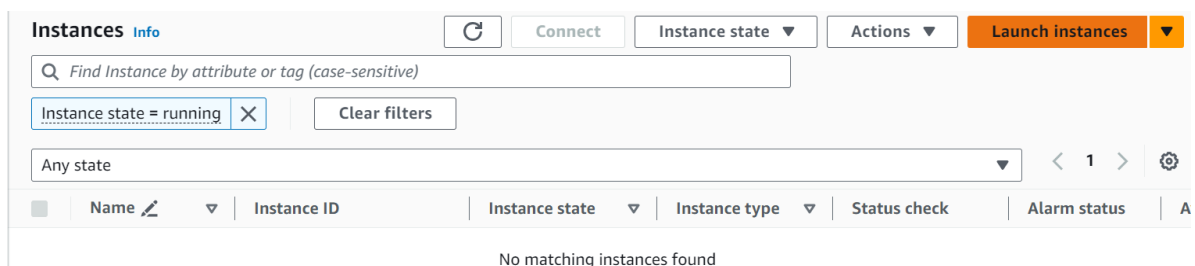
Step III : then Save Changes.



Launch Instances in Singapore region

1) LAUNCH PUBLIC INSTANCE

Step I : Go to EC2 service, Launch the instances in public subnet.



Step II : choose the key-pair, network settings and launch the instance.

▼ Network settings [info](#)

VPC - required [info](#)

vpc-036fab3c406b95854 (vpc-a)
10.0.0.0/16

Subnet [info](#)

subnet-00abb24f16b11e1a8 **pub_subnet**
VPC: vpc-036fab3c406b95854 Owner: 767397909313
Availability Zone: ap-southeast-1a IP addresses available: 251
CIDR: 10.0.0.0/24

Auto-assign public IP [info](#)

Enable

Firewall (security groups) [info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

launch-wizard-1

Source type [info](#) Source [info](#) Destination [info](#)

Anywhere e.g. SSH for admin desktop

Security group rule 2 (ICMPv4, 0.0.0.0/0)

Type [info](#) Protocol [info](#) Port range [info](#)

All ICMP - IPv4 ICMP All

Source type [info](#) Source [info](#) Description - optional [info](#)

Custom e.g. SSH for admin desktop

► Advanced network configuration

▼ Summary

Number of instances [info](#)

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more
ami-0144b0a0b0b01

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

2) LAUNCH PRIVATE INSTANCE

Step I : Launch another Instance in the Private subnet.

vpc-036fab3c406b95854 (vpc-a)
10.0.0.0/16

Subnet [info](#)

subnet-049f4cb67e14c9f16 **pri_subnet**
VPC: vpc-036fab3c406b95854 Owner: 767397909313
Availability Zone: ap-southeast-1b IP addresses available: 251
CIDR: 10.0.1.0/24

Auto-assign public IP [info](#)

Disable

Firewall (security groups) [info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups [info](#)

Select security groups

sg-0ab3955cc2ee18b24
vpc-036fab3c406b95854

Launch instance

Step II : follows similar steps as for the public instance.

3) CONFIGURE SECURITY GROUP RULES

Step I : Edit Inbound rules for both the instances in Security group.

Step II : Add all ICMP in anywhere in both security groups.

Source type	Source	Description - optional
Anywhere	<input type="text" value="Add CIDR, prefix list or secur"/> <input type="text" value="0.0.0.0/0"/>	<input type="text" value="e.g. SSH for admin desktop"/>
<div> ▼ Security group rule 2 (ICMP, All, 0.0.0.0/0) Remove </div>		
Type	Protocol	Port range
All ICMP - IPv4	ICMP	All
Source type	Source	Description - optional
Custom	<input type="text" value="Add CIDR, prefix list or secur"/> <input type="text" value="0.0.0.0/0"/>	<input type="text" value="e.g. SSH for admin desktop"/>

4)CONNECT THE INSTANCES

Step I : Connect to the public Instance.

```
#_
~\###_ Amazon Linux 2023
~~\_#####\
~~\####|
~~\#/ https://aws.amazon.com/linux/amazon-linux-2023
~~v~' '->
~~~
~~.-. /
~/m/'
```

[ec2-user@ip-10-0-0-105 ~]\$

Ping the private instance .

Step I : In paris region ,go to VPC service.

Your VPCs (1) [Info](#)

Q Search

< 1 > ⚙

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	-	vpc-07fca39cb1e6ce835	Available	172.31.0.0/16	-

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

vpc-2

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

20.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Step II : click on create VPC with the name and IPv4 CIDR and click on create.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

Q Name

Q vpc-2

Remove tag

Add tag

You can add 49 more tags

Cancel

Create VPC

Step III : Automatically,route table is created give its name.

Route tables (1/2) [Info](#) Refresh Actions Create route table

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations
<input checked="" type="checkbox"/>	- Edit Name	-0d0bdf2fc9d9f7c94	-	-
<input type="checkbox"/>	- <input type="text" value="vpc-2"/>	-0ff53a715a3fd046d	-	-

Cancel Save

2)CREATE SUBNET IN PARIS REGION

Step I : Go to Subnets, click on create Subnets.

Subnets (3) [Info](#) Refresh Action

<input type="checkbox"/>	Name	Subnet ID	State
<input type="checkbox"/>	-	subnet-08260fcce86a72083	✓ Available
<input type="checkbox"/>	-	subnet-0109d8bb0afcdfa1a	✓ Available
<input type="checkbox"/>	-	subnet-07eea96c02e2478e9	✓ Available

Step II : Create the private subnet in Paris region follows the step as in Singapore region.

[VPC](#) > [Subnets](#) > [Create subnet](#)

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

Associated VPC CIDRs

IPv4 CIDRs

20.0.0.0/16

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block

256 IPs

▼ Tags - optional

Key

×

Value - optional

×

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

► AWS Command Line Interface command

Cancel

Create subnet

Launch Instance in Paris region

3) LAUNCH PRIVATE INSTANCE IN PARIS REGION

Step I : Go to in EC2 Service, click on launch Instance.

Step II : Give the name to instance and all needed things.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-06bcdc6faa3c78ce (vpc-2)
20.0.0.0/16

Subnet [Info](#)

subnet-0ab82143a558d3469 pri_subnet
VPC: vpc-06bcdc6faa3c78ce Owner: 767397909313
Availability Zone: eu-west-3a IP addresses available: 251 CIDR: 20.0.0.0/24

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Step III : In Security group, add inbound rule All ICMP .

ssh TCP 22

Source type [Info](#) Source [Info](#) Description - optional [Info](#)

Anywhere [Add CIDR, prefix list or security group](#) e.g. SSH for admin desktop

0.0.0.0/0

▼ Security group rule 2 ICMP: All, 0.0.0.0/0

Type [Info](#) Protocol [Info](#) Port range [Info](#)

All ICMP - IPv4 ICMP All

Source type [Info](#) Source [Info](#) Description - optional [Info](#)

Custom [Add CIDR, prefix list or security group](#) e.g. SSH for admin desktop

0.0.0.0/0

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend restricting access to only the allowed source IP addresses.

Summary

Number of instances [Info](#)

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.3.2...read more

ami-0b73b046faa4dc7f8

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

Cancel Launch instance

Step IV : Launch it.

Set up the VPC Peering

1)CREATE PEERING CONNECTION

Step I : Go to Singapore region and click VPC.

Step II : Click on Peering Connections and then click on create Peering Connections.

Peering connections

[Info](#)

Actions

Find resources by attribute or tag

Name	Peering connection ID	Status
No peering connection found		

Step III : Give the name, then Select the requester id, another region as our VPC in paris then Copy the VPC ID of paris and Paste it.

Peering connection settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

vpc_1tovpc_2

Select a local VPC to peer with

VPC ID (Requester)

vpc-036fab3c406b95854 (vpc-a) ▼

VPC CIDRs for vpc-036fab3c406b95854 (vpc-a)

CIDR	Status	Status reason
10.0.0.0/16	✔ Associated	-

10.0.0.0/16

✔ Associated

Select another VPC to peer with

Account

☒ My account

☐ Another account

Region

☐ This Region (ap-southeast-1)

☒ Another Region

Europe (Paris) (eu-west-3) ▼

VPC ID (Acceptor)

vpc-06bcbdc6faa3c78ce

Step IV : Then, Click on create Peering Connections.

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional

Q Name X Q vpc_1tovpc_2 X Remove

Add new tag

You can add 49 more tags.

Cancel Create peering connection

2)ACCEPT PEERING CONNECTION

Step I : Go to Paris region in Peering Connections, select the connection and click on actions then click on accept request.

Peering connections (1/1) Info

Find resources by attribute or tag

Name	Peering connection ID	Status
-	pcx-0bccc212a25424d85	Pe...

Actions

- View details
- Accept request
- Reject request
- Edit DNS settings
- Manage tags
- Delete peering connection

Create peering connection

Step II : request accepted ,status is Provisioning.

Peering connections (1) Info

Find resources by attribute or tag

Name	Peering connection ID	Status
-	pcx-0bccc212a25424d85	Provisioning

3)UPDATE ROUTE TABLES FOR PEERING CONNECTION

Step I : In Paris ,Go to the Subnet click on subnet ID ,copy the CIDR and Go back to Singapore region and click on route tables.

[VPC](#) > [Route tables](#) > [rtb-0d0bdf2fc9d9f7c94](#) > [Edit routes](#)

Edit routes

Destination	Target	Status	Propagate
20.0.0.0/16	local	✓ Active	No
<input type="text" value="10.0.1.0/24"/>	<input type="text" value="local"/>		
	Peering Connection	-	No
	<input type="text" value="pcx-0bccc212a25424d85"/>		
<input type="button" value="Add route"/>			

Cancel

Step II : click on edit route the add route paste this CIDR in destination and choose the peering connections and the save Changes.

[VPC](#) > [Route tables](#) > [rtb-0d258307fecddd287](#) > [Edit routes](#)

Edit routes

Destination	Target	Status	Propagate
10.0.0.0/16	local	✓ Active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="local"/>		
	Internet Gateway	✓ Active	No
	<input type="text" value="igw-05823b44bf3fe9eaa"/>		
<input type="text" value="20.0.0.0/24"/>	Peering Connection	-	No
	<input type="text" value="pcx-0bccc212a25424d85"/>		
<input type="button" value="Add route"/>			

Cancel

Step III : Now , go to the subnet of Singapore region of private Subnet.

Step IV : Copy the CIDR and go to paris region in route table, click on edit and the add rule and paste CIDR and select the peering connections and then save changes.

Cancel

Add route

10.0.1.0/24	bcx-0pcccc5j5952454982	X	
	Peering connection	▲	-
	local	X	
50.0.0.0/16	local	▲	Active
Destination	Target	Status	Propagated

Edit routes

[ABC](#) > [Route tables](#) > [rtb-0b0b9bf5fca9b9f7c94](#) > Edit routes

4)CHECK CONNECTION

Step I : now copy the private IP of Private Instance and ping it on connected instance.

Step II : It is Pinged Successfully, It means Peering Connection is done.

```
#  
~#  
~\#####\  
~\#####\  
~\#####\  
~\##/  
~V~' '~>  
~.  
~_./_____  
~/m/'
```

Amazon Linux 2023

<https://aws.amazon.com/linux/amazon-linux-2023>

```
[ec2-user@ip-10-0-1-84 ~]$ ping 20.0.0.243  
PING 20.0.0.243 (20.0.0.243) 56(84) bytes of data:  
64 bytes from 20.0.0.243: icmp_seq=1 ttl=127 time=166 ms  
64 bytes from 20.0.0.243: icmp_seq=2 ttl=127 time=166 ms  
64 bytes from 20.0.0.243: icmp_seq=3 ttl=127 time=166 ms  
64 bytes from 20.0.0.243: icmp_seq=4 ttl=127 time=166 ms  
64 bytes from 20.0.0.243: icmp_seq=5 ttl=127 time=166 ms
```

PublicIPs: 3.0.16.245 PrivateIPs: 10.0.0.105

Step IV: Copy the private key of private instances and paste it in vim key.pem and give the rw permission.

Step V: to give remote access of private instance give command `ssh -i "keyname" ec2-user@privateIP`.

Step VI : here ,we can remotely access the private IP.

[illegible]

PublicIPs: 3.0.16.245 PrivateIPs: 10.0.0.105